PART 1 – PLAN OF INSTRUCTION/LESSON PLAN	
INSTRUCTOR:	**SHELL AUTHOR: HQ AF/XOS-FI (Mr. Bruce L. Kilgore DSN 425-0008)**
SUBJECT: Initial Security Education Orientation For Cleared Personnel	**DATE: 18 May 2005** **TIME:** (2 Hours)

I. OBJECTIVE: The objective of this lesson is for each cleared military member and civilian employee to be knowledgeable of the responsibilities and roles in the Air Force Information Security Program. (NOTE: Supervisors are encouraged to personalize this lesson plan and tailor it to meet local needs.) Each student will:

1. Know the basic information security policy and principles of program management.
2. Know the marking and safeguarding requirements for protecting classified and unclassifed controlled information.
3. Understand the principles for handling foreign government information.
4. Know when prior personnel security investigations and/or determinations are acceptable for granting access to classified information.
5. Know the minimum elements of information that must be provided to individuals upon initial indoctrination for access to NATO classified information.
6. Understand their responsibilities for derivatively classifying information.

II. SUPPORT MATERIAL AND GUIDANCE:

Audio Visual Aids: N/A
Training Equipment: N/A
Training Method: Lecture/Demonstration.
Instructor Study References:

1. AFI 31-401, *Information Security Program Management*. (This lesson plan may be used by the supervisor to provide continuing Security Education/Refresher Training.)
2. Executive Order 12958 as amended
3. 32 CFR Part 2001 Information Security Oversight Office (ISOO), Classified National Security Information, 13 Oct 1995 5. DOD 5200.1-R
4. USSAN 1-69

PRESENTATION: The instructor will discuss principles of Information Security and provide an initial orientation identified in AFI 31-401, Attachment 7.

APPLICATION/EVALUATION: Determined locally

INSTRUCTOR REQUIREMENTS: One instructor is required to conduct the lecture

SUPERVISOR APPROVAL AND DATE	
DATE: **SIGNATURE:**	**DATE:** **SIGNATURE:**

PART II

CLEARED PERSONNEL INITIAL TRAINING

(March 1, 2005)

INTRODUCTION

This standard lesson plan contains the minimum elements of information that must be provided to individuals with a clearance upon arrival at any duty assignment. The supervisor or security manager must tailor this lesson plan to ensure cleared personnel are knowledgeable of their security responsibilities as related to their jobs and the organization's mission.

Using the elements of attention, motivation and overview; introduce the subject of Initial Security Orientation for cleared personnel.

BODY

PRESENTATION

Objective: Provide a tailored initial security orientation, including the mandatory NATO briefing and derivative classification training, to cleared personnel. Trainees will gain basic knowledge of the information security program. (References: Executive Order 12958; 32 CFR Part 2001, Information Security Oversight Office (ISSO), Classified National Security Information; AFI 31-401; AFI 31-403; AFPD 31-4; USSAN 1-69.)

All personnel in the organization who are cleared for access to classified information must receive an initial orientation to the Information Security Program before being allowed access to classified information. This initial orientation is intended to produce a basic understanding of the nature of classified information and the importance of its protection to the national security. It places cleared personnel on notice of their responsibility to play a role in the security program, and provides them enough information to ensure proper protection of classified information in their possession. Additionally, completion of this training satisfies the requirement for all Air Force personnel to receive an initial access briefing on the NATO security program. Supervisors and security managers must address as a minimum the material identified in the "Topic" column. The "Personalization" column includes suggested minimum discussion on each topic; however, the lesson must be tailored to meet the needs of the member's duties. This lesson plan may be used by the supervisor to provide continuing Security Education/Refresher Training.

TOPIC	PERSONALIZATION
ROLES AND RESPONSIBILITIES	
1. IDENTIFY THE SENIOR AND LOCAL AIR FORCE OFFICIAL AND SECURITY PERSONNEL AND THEIR RESPONSIBILITIES?	A. The Senior Air Force Official for protection of classified information is the Administrative Assistant to the Secretary (SAF/AA). This office provides broad general policy and designates positions as Secret and Confidential Original Classification Authorities. B. Specific policies and procedures for information security are developed by the Chief, Information Security Division, Directorate of Security Forces and Force Protection, Directorate of Strategic Security, Deputy Chief of Staff/Air and Space Operations (HQ USAF/XOS-FI). This office serves as the ISPM link to SAF/AA and OSD security policy staff members as well as providing oversight of the MAJCOM ISPM. C. Policy is further refined by the MAJCOM Director of Security Forces who prescribes MAJCOM unique requirements and provides oversight of the installation level ISPM. D. Policy is implemented at the local level by the Information Security Program Manager, normally the base Chief of Security Forces. This office develops installation specific policy and procedures and provides support services for the security manager. Additionally, this office conducts a Program Review of each organization on an annual basis. E. Each commander appoints a security manager and alternate to implement and manage the program within the unit. F. Your security manager is: _____, This person develops a unit operating instruction with specific security procedures and is the focal

TOPIC	PERSONALIZATION
	point for all information and personnel security issues. G. Your alternate is: _____. The alternate is ready to assist during the security manager's absence. In the case of questions or concerns about security matters you should contact your security manager or alternate.
2. KNOW THE RESPONSIBILITIES OF AIR FORCE PERSONNEL WHO CREATE OR HANDLE CLASSIFIED INFORMATION?	A. The Original Classification Authority (OCA) determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism. AF OCAs are appointed by the Secretary of the Air Force or the Administrative Assistant to the Secretary. The OCAs are responsible to: • Publish classification and declassification guides to facilitate the proper and uniform derivative classification and declassification of their information. • Each OCA will revise their security classification guides to include an advisory statement in the Release of Information section. • Know the eight subject areas prescribed by Executive Order 12958 that may result in classification are: o Military plans, weapons systems or operations o Foreign government information o Intelligence activities (including special activities), intelligence sources or methods, cryptology o Foreign relations or foreign activities of the U.S., including confidential sources; o Scientific technological or economic matters relating to the national

TOPIC	PERSONALIZATION
	security, which includes defense against transnational terrorism; o U.S. Government programs for safeguarding nuclear materials and facilities o Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism o Weapons of mass destruction B. OCAs must: • Before original classification decisions are made, determined that classification guidance is not already available in the form of classification guides, plans or other memoranda. • Know that decisions to classify information have a substantial impact on the operations of the Air Force. Others who work with the information use these original decisions to make proper derivative classification decisions and to assure that the information is properly protected from unauthorized disclosure. • Understand they are accountable to the Secretary of Defense for their classification decisions. • Exercise a substantial degree of autonomy in operations or mission. Information warranting original classification must be developed in the normal course of operations or activity. In those rare cases where the OCA's determination must be rendered verbally due to the priorities of an on-going operation, written confirmation will be issued within seven(7) calendar days. • Document original classification decisions clearly and concisely in writing. This may be in the form of a memorandum, plan, order or letter of issuance of a security classification guide (SCG). A SCG must be issued for

each system, operation, program, or project in which classified information is involved.

- Absent a SCG, must exercise this authority an average of twice a year to justify and retain designation as an OCA.
- Notify users when there are changes to an original classification decision. Classification may change as each phase in an operation or research and development cycle occurs.
- Ensure that a security review for possible declassification is conducted expeditiously in the event of compromise, formal challenges to classification, classification conflicts, and requests from individuals who are not OCAs, but who believe they have originated information requiring classification by an OCA. Requests from individuals who are not OCAs, but believe they have originated information requiring classification by an OCA shall be decided within 30 days of receipt.
- Be prepared to present, as required, deposition and expert testimony in courts of law concerning classification of national security information and be prepared to defend and justify their original classification decisions in court and as required by law or regulation.
- Develop, as appropriate, automatic declassification/systematic declassification guidance for use in review of records that are of permanent historical value and 25 years old or older. This guidance shall be published in the appropriate security classification guide or in a declassification guide whenever appropriate.

C. Derivative classifier (any cleared AF person) must:

- Be knowledgeable of where to attain classified guidance.

TOPIC	PERSONALIZATION

	• Know and document the level of classification, duration of classification and the source of classified information that is included in the document, e-mail, briefing, etc., that they are generating:
	  o Know how to apply classification markings
	  o Know how to use a security classification guide or other derivative source
	  o Know how to safeguard classified information
	  o Observe and respect the original classification decision
	  o Know how to challenge classification decisions
	  o Know they are accountable for the accuracy of their work
	  o Understand how to use tentative classification provisions
	  o Understand how to downgrade or declassify information as an authorized holder of the information in accordance with the direction of the cognizant OCA or classification guide
	• Maintain a list of sources with the record copy when multiple sources of classified are used.
	• Know that derivative classification is:
	  o Extracting, paraphrasing, restating or generating classified information
	  o Based on a security classification guide or one or more source documents or both
	• Know the authorized types of sources that can be used for derivative classification.
	• Know that a security classification guide:
	  o Is a collection of precise and comprehensive guidance regarding specific program, system, operation, or weapon system elements of information to be classified, including the classification levels,

TOPIC	PERSONALIZATION
	○ reasons for classification and the duration of classification ○ Is approved and signed by the cognizant original classification authority ○ Is an authoritative source for derivative classification ○ Ensures consistent application of classification to the same information • Know how and where to get security classification guidance ○ Check with the security manager and/or the program or project office ○ Check DOD 5200.1-I, *Index of Security Classification Guides*, accessible from the Defense Technical Information Center ○ In the case of a military operation and the creation/execution of plans and orders thereto, check the higher headquarters office that mandated or directed the operation/mission D. Everyone that handles classified information must: • Understand they are responsible, both personally and officially, for safeguarding classified information for which they have access. Collecting, obtaining, recording, or removing, for any unauthorized use whatsoever, of any sensitive or classified information, is prohibited. • Be aware that advancing technology provides constantly changing means to quickly collect and transport information. The introduction ofelectronic storage or transmission devices into areas that store, process, and/or generate classified information increases the risk to that information. • Know that all security infractions and/or violations must be immediately reported, circumstances examined and those responsible held accountable and appropriate

TOPIC	PERSONALIZATION
	corrective action taken. Commanders, equivalents, and staff agency chiefs are responsible for ensuring that personnel are knowledgeable and understand their responsibility to protect information and resources deemed vital to national security.
3. KNOW WHO TO CONTACT IN CASE OF QUESTIONS OR CONCERNS ABOUT SECURITY MATTERS?	A. Your Security Manager is: _____, who can be reached at _____. B. The Alternate Security Manager is: _____, who can be reached at _____. C. The Information Security Program Manager is: _____.
ELEMENTS OF CLASSIFYING AND DECLASSIFYING INFORMATION	
4. KNOW WHAT CLASSIFIED INFORMATION IS, AND WHY IS IT IMPORTANT TO PROTECT IT?	A. The U.S. Government and private industry have a uniform system for classifying, declassifying, and safeguarding national security information. This system recognizes that the interests of the United States and its citizens require that certain information concerning the national defense and foreign relations be protected against unauthorized disclosure. Information may not be classified unless its disclosure could reasonably be expected to cause damage to the national security. B. Classified information is inherently sensitive and damage to our national security may result if that information is compromised. The goal of the Information Security Program is to efficiently and effectively

protect Air Force information by delegating authority to the lowest levels possible; encouraging and advocating use of risk management principles; focusing on identifying and protecting only that information that requires protection; integrating security procedures into our business processes so that they become transparent; and, ensuring everyone understands their security roles and responsibilities

C. Protecting information is critical to mission accomplishment. The Secretary of the Air Force has established procedures to ensure that prompt and appropriate management action is taken in case of compromise of classified information, improper classification of information, violation of security policy and incidents that may put classified information at risk of compromise. The procedures focus on correction or elimination of the conditions that caused or occasioned the incident.

D. Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of classification authority. A report must be submitted through channels when someone knowingly, willfully, or neglectfully discloses classified information. Action may also be taken under the Uniform Code of Military Justice for violations of that Code and under applicable criminal law. DOD military and civilian personnel are subject to sanctions if they knowingly, willfully, or negligently:
   - Disclose to unauthorized persons properly classified information properly classified.
   - Improperly classify or continue the improper classification of information.
   - Create or continue an improper Special Access Program.
   - Violate any other security policy.

TOPIC	PERSONALIZATION
5. UNDERSTAND THE LEVELS OF CLASSIFIED INFORMATION AND THE DAMAGE CRITERIA ASSOCIATED WITH EACH LEVEL?	A. National security information is classified into three categories. Those categories and the damage associated with each category: • **Confidential** shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause ***damage*** to the national security that the original classification authority is able to identify or describe. • **Secret** shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause ***serious damage*** to the national security that the original classification authority is able to identify or describe. • **Top Secret** shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause ***exceptionally grave damage*** to the national security that the original classification authority is able to identify or describe.
6. KNOW WHAT CLASSIFICATION MARKINGS ARE TO BE USED AND WHY IS IT IMPORTANT THAT THEY BE PROPERLY APPLIED?	A. The purpose of classification markings is to: • Identify the exact information that requires protection • Indicate the level of classification assigned to the information • Provide guidance on downgrading and declassification • Give information on the source and reason for classification

TOPIC	PERSONALIZATION
	• Warn of special access, control, or safeguarding requirements B. Classified documents are required to have the following markings: • The overall classification of the document • The agency, office of origin, and date of the document • Identification of the source of classification of the information contained in the document and, for originally classified information, a concise reason for classification • Declassification instructions, and any downgrading instructions that apply • Identification of the specific classified information in the document and its level of classification (page and portion markings) • Control notices and other markings that apply to the document
DERIVATIVE CLASSIFICATION	
7.a. KNOW WHAT DERIVATIVE CLASSIFICATION IS.	A. Derivative classification is the act of incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information. The source information ordinarily consists of a classified document or a classification guide issued by an OCA. B. Within DOD, all cleared personnel can perform derivative classification. (NOTE: Does not apply to RD and FRD)
7.b. KNOW THE AUTHORIZED TYPES OF SOURCES THAT CAN BE USED FOR DERIVATIVE CLASSIFICATION.	

TOPIC	PERSONALIZATION
	A. Use only authorized sources of instructions about the classification of the information in question. Authorized sources of instructions about classification are security classification guides, other forms of classification guidance, and markings on material from which the information is extracted. B. The use of only memory or "general rules" about the classification of broad classes of information is prohibited.
7.c. KNOW WHERE TO ATTAIN CLASSIFICATION GUIDANCE.	A. Your security manager should identify sources of classification guidance routinely used in the performance of your duties. B. Guides are also available from the DTIC web site. To access the DTIC web site you must have a DTIC account. The URL for this is http://www.dtic.mil/dtic/registration.
7.d. KNOW WHAT A CLASSIFICATION GUIDE PROVIDES.	A. Identify the subject matter of the classification guide. B. Identify the original classification authority by name or personal identifier, and position. C. Identify an agency Point of Contact (POC) (name, office symbol, mailing address, organizational e-mail address, DSN/commercial phone numbers) for questions regarding the classification guide. D. Provide the date of issuance or last review. E. State precisely the categories or elements of information to be declassified, to be downgraded, or not to be declassified. F. State which classification level applies to each element of information, and, when useful, specify the elements of information that are unclassified.

TOPIC	PERSONALIZATION
	G. State a concise reason for classification which, at a minimum, cites the applicable classification category or categories. H. State, when applicable, special handling caveats, to include foreign disclosure control markings. I. Prescribe declassification instructions for each element of classified information. J. Identify any related files series that have been exempted from automatic declassification. K. To the extent a guide is used in conjunction with the automatic declassification provisions state precisely the elements of information to be exempted from declassification to include: • The appropriate exemption category. • A date or event for declassification.
7.e. KNOW HOW TO APPLY CLASSIFICATION MARKINGS.	A. Use caution when paraphrasing or restating information extracted from a classified source document to determine whether the classification may have been changed in the process. B. Take appropriate and reasonable steps to resolve doubts or apparent conflicts about the classification, level of classification, and duration of classification of information. These steps may include consulting a security classification guide or referral to the organization responsible for the original classification. In cases of apparent conflict between a security classification guide and a classified source document about a discrete item of information, the instructions in the security classification guide shall take precedence.
7.f. KNOW HOW TO USE A SECURITY CLASSIFICATION GUIDE OR OTHER DERIVATIVE SOURCE.	A. Carefully analyze the material you are classifying to determine what information

TOPIC	PERSONALIZATION
	it contains or reveals and evaluate that information against the instructions provided by the classification guidance or the markings on source documents. B. Portion mark your drafts and keep records of the sources you use, to facilitate derivative classification of the finished product. C. Bring forward markings from the source document or classification guide. Identify the classification source on the "Derived From" line; including the agency, office of origin, and date of the source or guide**.** D. When material is derivatively classified based on "multiple sources" (more than one security classification guide, classified source document, or combination thereof), the you must compile a list of the sources used. A copy of this list must be included in or attached to the file or record copy of the document.
7.g. KNOW HOW TO CHALLENGE CLASSIFICATION DECISIONS.	A. If you believe that information is improperly or unnecessarily classified, communicate that belief to you security manager. This may be done informally or by submission of a formal challenge to the classification as provided for in E.O. 12958 (reference (e)). Informal questioning of classification is encouraged before resorting to formal challenge. B. All classified information undergoing a challenge or a subsequent appeal will remain classified until a final resolution is reached.
7.h. UNDERSTAND HOW TO USE TENTATIVE CLASSIFICATION PROVISIONS.	A. Mark and protected the document as if it is classified. B. Forward it through the chain-of-command to the appropriate Original

TOPIC	PERSONALIZATION
	Classification Authority. A list of OCAs is available from your ISPM.
7.i. UNDERSTAND HOW TO DOWNGRADE OR DECLASSIFY INFORMATION IN ACCORDANCE WITH THE DIRECTION OF THE OCA OR CLASSIFICATION GUIDE.	A. Information may be downgraded by any official who is authorized to classify or declassify the information. B. When a document or item of material is marked for downgrading or declassification on a date or event, the downgrading or declassification is automatic at the specified time unless word to the contrary has been received from the originator or other authority. C. If a holder of the material has reason to believe it should not be downgraded or declassified, he or she shall notify the originator through appropriate administrative channels. D. The document or material shall continue to be protected at the originally assigned level of classification until the issue is resolved. E. When a document is declassified automatically in accordance with declassification markings appearing on it, the overall and page markings on the document should be canceled F. If a document is downgraded in accordance with its markings, cancel the old classification markings and substitute the new ones. As a minimum, the markings on the cover (if one exists), title page (if one exists), and the first page must be changed. G. If a document is declassified or downgraded earlier than indicated by its markings, the rules for remarking in paragraph C5.5.1., above, must be followed. In addition, place the following information on the document: • The date of the downgrading or declassification remarking.

TOPIC	PERSONALIZATION
	• The authority for the action (e.g., the identity of the original classifier who directed the action, or identification of the correspondence or classification instruction that required it). When possible, file a copy of the correspondence authorizing the downgrade or declassification with the document.
8. KNOW THE GENERAL REQUIREMENTS FOR DECLASSIFYING INFORMATION?	A. Within the Air Force, only OCAs have the authority to declassify or downgrade classified information. At the time an item of information is classified, original classifiers will determine which of the following four declassification instructions will be used, selecting whenever possible, the declassification instruction that will result in the shortest duration of classification. • A date or event less than 10 years from the date of the document; or, if unable to identify such a date or event; • A date or event less than 10 years from the date of the document; or, if unable to identify such a date or event • A date 10 years from the date of the document; or • A date greater than 10 and less than 25 years from the date of the document; or • A date 25 years from the date of the document. B. When a document has been declassified, the following markings are applied • The word, "Declassified • The authority for the action (the identity of the OCA who directed the action, or identification of the correspondence or classification instruction that required it)

TOPIC	PERSONALIZATION
	• The date of declassification • The overall classification markings that appear on the cover page or first page shall be marked through with a straight line
9. KNOW THE PROCEDURES FOR CHALLENGING THE CLASSIFICATION STATUS OF INFORMATION?	A. If you believe that information is improperly or unnecessarily classified, communicate that belief to you security manager. This may be done informally or by submission of a formal challenge to the classification as provided for in E.O. 12958 (reference (e)). Informal questioning of classification is encouraged before resorting to formal challenge. B. All classified information undergoing a challenge or a subsequent appeal will remain classified until a final resolution is reached.
ELEMENTS OF SAFEGUARDING	
10. WHAT ARE THE PROPER PROCEDURES FOR SAFEGUARDING CLASSIFIED INFORMATION?	A. The Air Force has a system of control measures to ensure that access to classified information is limited to authorized persons. The system includes administrative, physical, and personnel control measures specific for the level of classification being protected. B. Classified information must be protected at all times either by storage in an approved device or facility or having it under the personal observation and control of an authorized individual. C. Classified material removed from storage shall be kept under constant surveillance of authorized persons. D. There shall be no external mark revealing the level of classified information authorized

TOPIC	PERSONALIZATION
	to be or actually stored in a given container or vault or to the priority assigned to the container for emergency evacuation and destruction. E. Classified document cover sheets (Standard Forms 703, 704 and 705) will be placed on classified documents not in secure storage. F. Classified information shall be discussed in telephone conversations only over secure communications circuits approved for transmission of information at the specific level of classification. G. Weapons or sensitive items such as funds, jewels, precious metals or drugs shall not be stored in the same container used to safeguard classified information. H. Documents and other material containing classified information shall be reproduced only when necessary for accomplishment of the organization's mission or for compliance with applicable statutes or directives. I. Classified documents and other material are retained only if they are required for effective and efficient operation of the organization or if their retention is required by law or regulation. Documents that are no longer required for operational purposes are disposed of in accordance with the provisions of the Federal Records Act (44 U.S.C. Chapters 21, 31 and 33, reference (p)). Material that has been identified for destruction is protected, as appropriate, for its classification until it is actually destroyed. Destruction of classified documents and material is accomplished by means that eliminate risk of reconstruction of the classified information they contain. Each activity with classified holdings establishes at least one day each year when specific attention and effort is focused on disposition of unneeded classified material ("clean-out day").

TOPIC	PERSONALIZATION
11. WHAT CONSTITUTES A COMPROMISE OF CLASSIFIED INFORMATION AND WHAT ARE THE PENALTIES ASSOCIATED WITH COMPROMISES?	A. Definition: The known or suspected exposure of clandestine personnel, installations, or other assets or of classified information or material, to an unauthorized person. B. DOD military and civilian personnel shall be subject to sanctions if they knowingly, willfully, or negligently: • Disclose to unauthorized persons properly classified information. • Improperly classify or continue the classification of information • Sanctions include, but are not limited to, warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of classification authority. Action may also be taken under the Uniform Code of Military Justice for violations of that Code and under applicable criminal law.
12. WHAT ARE THE GENERAL CONDITIONS AND RESTRICTIONS FOR ACCESS TO CLASSIFIED INFORMATION?	A. No person may have access to classified information unless that person has been determined to be trustworthy and access is essential to the accomplishment of a lawful and authorized Government purpose. • Clearance • Training • Signed NdA • Need-to-Know B. Everyone who has been granted access to classified information is responsible for

TOPIC	PERSONALIZATION
	providing protection to information and material in their possession or control that contains such information.
13. WHAT SHOULD AN INDIVIDUAL DO WHEN HE OR SHE BELIEVES SAFEGUARDING STANDARDS HAVE BEEN VIOLATED?	A. If you find classified material out of proper control, take custody and safeguard the material, if possible, and immediately notify your supervisor, security manager or commander. B. If you become aware of the possible compromise of classified information, immediately report it to your supervisor, security manager, or commander. C. If classified information appears in the public media, be careful not to make any statement or comment that would confirm the accuracy or verify the classified status of the information. Report the matter to your supervisor, security manager or commander, but do not discuss it with anyone without an appropriate security clearance and need-to-know. If approached by a representative of the media who wishes to discuss information you believe is classified, neither confirm nor deny the accuracy of or the classification of the information, and report the situation immediately to your supervisor, security manager or commander and public affairs authorities.
14. WHAT STEPS SHOULD BE TAKEN IN AN EMERGENCY EVACUATION SITUATION?	A. Every organization develops appropriate plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, civil disturbance, terrorist activities, or enemy action, to minimize the risk of its compromise. Review the local procedures with the trainee.

TOPIC	PERSONALIZATION
	B. The level of detail and amount of testing and rehearsal of these plans are locally determined by an assessment of the risk of hostile action, natural disaster, or terrorist activity that might place the information in jeopardy.
15. WHAT ARE THE APPROPRIATE POLICIES AND PROCEDURES FOR TRANSMISSION OF CLASSIFIED INFORMATION?	A. The Department of Defense (DOD) utilizes a risk management approach to the transmission and transportation of classified information and materials. This approach emphasizes the protection of information in a cost-effective manner. B. Policy guidance for transmission and transportation of classified information is contained in DOD5200.1-R and AFI 31-401. The Third Agency Rule states classified information originating in a department or agency other than DOD will not be disseminated outside DOD without the consent of the originating department or agency. C. Classified material needs to be prepared for shipment, packaged, and sealed in ways that minimize risk of accidental exposure or undetected, deliberate compromise. D. When classified information is transmitted via an appropriate carrier, it needs to be enclosed in two opaque, sealed envelopes, wrappings, or containers, durable enough to properly protect the material from accidental exposure and facilitate detection of tampering. E. A receipt must be utilized for Top Secret and Secret classified information. Receipts for Confidential classified information are only required if the sender deems it necessary. Receipts must identify the sender, the addressee and the document. F. DOD personnel must ensure documents are packaged so that classified text is not in

TOPIC	PERSONALIZATION
	direct contact with the inner envelope or container. G. The outer envelope or container for classified material needs to be addressed to an official government activity or to a DOD contractor with a facility clearance and appropriate storage capability. The envelope should show the complete return address of the sender. The inner envelope or container needs to show the address of the receiving activity, the address of the sender, the highest classification of the contents and any applicable special instructions. H. Top Secret information is transmitted only when there is proper clearance level, access is necessary for the job and the recipient has the need-to-know. • Direct contact between appropriately cleared persons. • Cryptographic Transmission System authorized by the Director, National Security Agency (NSA), or a protected distribution system designed and installed to meet the requirements of National Communications Security Instruction 4009 can be used. • Defense Courier Service (DCS). DCS operates an international network of couriers and courier stations for the expeditious, cost-effective and secure transmission of qualified classified documents and material. • The Department of State Diplomatic Courier Service. Use of this service must be coordinated with the Department of State in advance. • Cleared U.S. military personnel and Government civilian employees specifically designated to carry the information traveling on a conveyance owned, controlled, or chartered by the U.S. Government; for example, on military flights. • Cleared U.S. military personnel and Government civilian employees specifically designated to carry the

information traveling on a scheduled commercial passenger aircraft within and between the United States, its Territories, and Canada.
- Cleared U.S. military personnel and Government civilian employees specifically designated to carry the information traveling on a scheduled commercial passenger aircraft on flights outside the Unites States, its Territories, and Canada.

I. Secret information may be transmitted by:
- Any of the means approved for the transmission of Top Secret information (except for certain limitations with the Defense Courier Service [DCS]); and
- Appropriately cleared contractor employees provided that the transmission meets the requirements specified in the NISPOM
- **U.S. Postal Service:** The various options for transmitting Secret information via the U.S. Postal Service include:
  - **Registered mail** within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico is the most secure service option offered by the Postal Service. It provides added protection for valuable and important mail. Registered articles are placed under tight security from the point of mailing to the point of delivery
  - **Express mail**, the Postal Service's fastest service within and between the 50 States, the District of Columbia, and the Commonwealth of Puerto Rico can be used. However, the "Waiver of Signature and Indemnity" block on the U.S. Postal Service Express Mail Label 11-B may not be executed under any circumstances. The use of external (street side) Express Mail collection boxes is prohibited.

TOPIC	PERSONALIZATION
	• Another means of transmission for Secret information is military postal service facilities. This service may be utilized for transmitting Secret information subject to the following condition: U.S. Postal Service registered mail can pass through Army, Navy, or Air Force Postal Service facilities outside the United States and its Territories, provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection. • Canadian registered mail can also be used to transmit Secret information using registered mail receipts between U.S. Government and Canadian Government installations in the United States and Canada. • Protective Security Service (PSS) carriers are cleared under the NISP to maintain constant surveillance of a shipment during transportation, including stops en route. PSS is authorized only within the Continental United States (CONUS) when other methods are impractical. PSS is normally utilized for shipping large quantities of material or for shipping bulk material that would be difficult or impractical to ship via other authorized means such as the U.S. Postal Service. • Secret classified information may be transported aboard Government and Government contract vehicles including aircraft, ships of the U.S. Navy, civil service-operated U.S. Naval ships, and ships of U.S. registry. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are U.S. citizens may be designated as escorts provided the control of the

carrier is maintained on a 24-hour basis. For private industry, escorts must be a cleared employee. The escort shall protect the shipment at all times, through personal observation or authorized storage, to prevent inspection, tampering, pilferage, or unauthorized access. Observation of the shipment is not required during flight or sea transit, provided it is loaded into a compartment that is not accessible to any unauthorized persons or in a specialized, secure, safe-like container.

- **On an exception basis**, when an urgent requirement exists for overnight delivery of Secret information to a DOD component within the United States and its Territories, we may use the current holder of the General Services Administration (GSA) contract to deliver such information overnight for the Executive Branch. Federal Express, United Parcel Service, AirNet Systems, Airborne Express, Associated Global Systems, Cavalier Logistics Management, CorTrans Logistics, DHL Airways, and Menlo Worldwide Forwarding (formally Emery) are currently approved to provide overnight service within the U.S. and its territories for Secret classified information. Commercial Overnight Delivery Requirements:
  - The sender is responsible for ensuring that an authorized person will be available to receive the delivery and verify the correct mailing address.
  - The package may be addressed to the recipient by name.
  - The *release signature block* on the receipt label shall not be executed under any circumstances.
  - The use of external (street side) collection boxes is prohibited

TOPIC	PERSONALIZATION
	J. Confidential information may be transmitted by means approved for transmission of Secret information. Additional approved US Postal Service transmissions include: • U.S. Postal Service Registered Mail for: o Material to and from Fleet Post Office (FPO) or Army Post Office (APO) addressees located outside the United States and its Territories. o Material when the originator is uncertain that the addressee's location is within U.S. boundaries. • U.S. Postal Service Certified Mail for material addressed to DOD contractors or non-DOD agencies. Certified mail can be utilized because it provides proof of mailing and delivery of mail. The sender receives a mailing receipt at the time of mailing, and a record of delivery is kept at the recipient's post office. A return receipt to provide the sender with proof of delivery can also be purchased for an additional fee. Certified mail service is available only for First-Class Mail or Priority Mail. Certified mail service is not available for international mail. It does offer insurance protection. It cannot be used for confidential material addressed to DOD contractors or non-DOD agencies • U.S. Postal Service first class mail between DOD Component locations anywhere in the United States and its Territories. The outer envelope or wrapper needs to be endorsed: "POSTMASTER: RETURN SERVICE REQUESTED". K. Commercial carriers may be used for transmitting Secret and Confidential information within the following guidelines: • Within CONUS, commercial carriers that provide a Constant Surveillance Service (CSS). • In the custody of commanders or masters of ships of U.S. registry who are U.S.

TOPIC	PERSONALIZATION
	citizens. Confidential information shipped on ships of U.S. registry may not pass out of U.S. Government control. The commanders or masters must sign a receipt for the material and agree to: o Deny access to the Confidential material by unauthorized persons, including customs inspectors, with the understanding that Confidential cargo that would be subject to customs inspection will not be unloaded. o Maintain control of the cargo until a receipt is obtained from an authorized representative of the consignee. L. On occasion you may need to transport large amounts of classified information or bulky classified material. In these situations freight shipment may be the most effective or timely option. Procedures for the shipment of bulk classified material as freight include: • Provisions for shipment in closed vehicles when required • Appropriate notice to the consignee concerning the shipment • Procedures at transshipment activities • Actions to be taken in case of non-delivery or unexpected delay in delivery • Accompanied by escort (DOD contractors) M. Transmission of Classified Material to Foreign Governments. National security is generally defined as the national defense or the foreign relations of the United States. Sharing of classified information among foreign nations and international organizations has a direct impact on U.S. national security. Therefore, information is carefully scrutinized (by the United States Government at the national level in the case of contractor requests) and great care is exercised in transmitting classified information to foreign governments and international organizations.

TOPIC	PERSONALIZATION
	• Classified information must be formally approved for release to foreign governments and international organizations. Once information has been approved for release to a foreign government or international organization, we must then ensure that it is properly transmitted by means that ensure proper transfer between representatives of each government. All international transfers of classified material take place through government-to-government channels. • Control and accountability of classified material is maintained until the material is officially transferred to the intended recipient government through its Designated Government Representative. In urgent situations, appropriately cleared DOD personnel may be authorized to hand-carry classified material. . • Foreign Nationals working within or assigned to DOD activities must be specifically authorized to access specific classified information. For example, a foreign liaison officer from a military ally must be specifically authorized not only to a level of classification access but also to specific categories/types of information. N. The physical transfer of classified information can be accomplished through a variety of means. Some of the most common means include hand-carrying and couriers. Mission requirements often dictate the means for transmitting and transporting classified information. • A hand carrier is a cleared employee/member who occasionally hand carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the

personal possession of the hand carrier except for authorized overnight storage.

- A courier is a cleared employee/member whose principle duty is to transmit classified material to its overnight storage.
- An escort is a cleared employee/member who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

O. Appropriately cleared personnel must be authorized to courier, escort or hand carry classified material between locations when other means of transmission or transportation cannot be used. The commander establishes procedures to ensure that hand carrying of classified material is minimized and does not pose unacceptable risk to the information. Hand carrying classified material is authorized only for specific circumstances.

- The information is not available at the destination and is required by operational necessity or a contractual requirement.
- The information cannot be sent via a secure facsimile transmission or by other secure means.
- The hand carry has been authorized.
- The U.S. escort will hand carry aboard a U.S. carrier or a foreign carrier, if no U.S. carrier is available. The information will remain in the custody and physical control of the U.S. escort at all times.
- Arrangements have been made for secure storage at a U.S. Government or cleared U.S. contractor facility.

P. Individuals' hand carrying or couriering classified information must be informed of and acknowledge their security responsibilities. This may be satisfied by a

briefing or by requiring the individual to read written instructions that contain specific information.

- The courier is liable and responsible for the material being escorted. DOD contractors must possess ID with contractor's name as well as the employee's name and photo.
- The classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities, embassies or cleared U.S. contractor facilities must be used for overnight storage. Classified material shall not be stored in hotel safes.
- The material shall not be opened en route except in the circumstances described in DOD 5200.1-R, subparagraph 7-300.b.(8), (Dealing with customs officials).
- The classified material is not to be discussed or disclosed in any public place.
- The courier shall not deviate from the authorized travel schedule.
- In cases of emergency, the courier must take measures to protect the classified material.
- The courier is responsible for ensuring that personal travel documentation (passport, courier authorization, and medical documents, etc.) is complete, valid, and current.
- A receipt is not required for Confidential material.

Q. There is no assurance of immunity from search by the customs, police, and/or immigration officials of various countries whose border the hand carrier or courier may cross. If officials inquire into the contents of the consignment, the hand carrier or courier will need to present their orders and ask to speak to the senior customs, police and/or immigration official. This action is normally sufficient enough to pass the material through customs unopened.

However, if the senior official demands to see the actual contents of the package, it may be opened in his or her presence, but should be done in an area out of sight of the general public.

- Precautions need to be taken to show officials only as much of the contents as will satisfy them that the package does not contain any other item. The hand carrier or courier will need to ask the official to repack the material or assist in repacking it immediately upon completion of the examination. The senior customs, police and/or immigration official will be requested to provide evidence of the opening and inspection of the package. The official must seal the package and sign any shipping documents, if any, or courier certificate confirming that the package was opened. Both the addressee and the dispatching security officer need to be informed in writing of the opening of the material.
- Classified material being hand carried or couried will need to be inventoried. A copy of the inventory needs to be retained by the hand carrier's or courier's security office and the hand carrier or courier needs to carry a copy.
- Upon return, the hand carrier or courier must return all classified material in a sealed package or produce a receipt signed by the security officer of the addressee organization for any material that is not returned.

R. Responsible officials must provide a written statement to all individuals escorting or carrying classified material authorizing such transmission. This authorization statement may be included in official travel orders except for travel aboard commercial aircraft.

S. DD Form 2501, "Courier Authorization," may be used to identify appropriately cleared DOD military and civilian personnel who have been approved to hand carry

classified material except for travel aboard commercial aircraft. The following provisions apply to its use:

- The individual has a recurrent need to hand carry classified information.
- An appropriate official in the individual's servicing security office signs the form.
- Stocks of the form are controlled to preclude unauthorized use.
- The form is issued for no more than one year at a time. The requirement for authorization to hand carry will be reevaluated and/or revalidated on at least an annual basis, and a new form issued, if appropriate.
- The use of the DD Form 2501 for identification/verification of authorization to hand carry Sensitive Compartmented Information or special access program information needs to be in accordance with policies and procedures established by the official having security responsibility for such information or programs.

T. Handcarrying aboard commercial aircraft: Despite today's technology and the ability to easily transmit information around the globe, there are instances when classified information may need to be transported by hand carrier or courier via commercial aircraft. This mode of transporting classified information presents special risks and challenges that must be addressed.

- In order to facilitate the hand carrier's or courier's processing through airline ticketing, screening and boarding procedures, advance coordination should be made with airline and departure terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the terms of DOD and Federal Aviation Administration (FAA) guidance. During this coordination, specific advice should be

TOPIC	PERSONALIZATION
	sought regarding the nature of the documentation that will be required. • The individual designated as hand carrier or courier needs to be in possession of a DOD or contractor-issued identification card that includes a photograph, descriptive data, and signature of the individual. For DOD personnel, if the identification card does not contain date of birth, height, weight, and signature, these items must be included in the written authorization. • The hand carrier or courier needs to possess the original authorization letter and ensure that it is on letterhead stationary of the agency authorizing the carrying of the classified material. The authorization letter needs to be translated into the official language of all countries the courier will be traveling to. The courier needs to have sufficient authenticated copies to provide to each airline involved. They should process the ticket through the airline ticketing and boarding procedure in the same way as other passengers. The package or the carry-on luggage containing the classified information should be routinely offered for inspection for weapons. The letter should provide the following information: o Full name of the individual and his or her employing agency or company o Type of identification the individual will present (for example, Air Force Research Laboratory Identification Card No. 1234; ABC Corporation Identification Card No. 1234) o Description of the material being carried (for example, three sealed packages, 9" X 8" X 24", addressee and addresser) o Point of departure, destination, and known transfer points o Date of issue and an expiration date

TOPIC	PERSONALIZATION
	○ Name, title and signature of the official issuing the letter. Each package or carton to be exempt shall be signed on its face by the official who signed the letter ○ Name of the individual designated to confirm the letter of authorization, and that person's official U.S. Government telephone number • Activities must coordinate in advance with airport and airline security prior to hand carrying, couriering, or escorting classified, bulk material aboard commercial aircraft. The hand carrier, escort, or courier or their appointed representative must ensure the on-loading and off-loading of the classified information. Advance coordination with the individual airline and airport security services is necessary to accomplish this.
16. Know the appropriate policies and procedures for the destruction of classified information.	A. Classified documents and other material are retained within AF organizations only if they are required for effective and efficient operation of the organization or if their retention is required by law or regulation. B. Classified information identified for destruction must be destroyed completely to preclude recognition or reconstruction. Methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, mutilation, chemical decomposition or pulverizing. C. Specifications concerning appropriate equipment and standards for destruction of other storage media may be obtained from the General Services Administration.

TOPIC	PERSONALIZATION
NORTH ATLANTIC TREATY ORGANIZATION (NATO)	
17.a. WHAT IS NATO INFORMATION?	A. NATO information is information that has been generated by or for NATO, or member nation national information that has been released into the NATO security system. B. The protection of this information is controlled under the NATO security regulations, and access within NATO is determined by the holder, unless restrictions are specified by the originator at the time of release to NATO.
16.b. MATERIAL RECEIVED FROM ANOTHER NATO MEMBER COUNTRY.	A. Material received by an agency direct from another NATO member nation may contain either NATO information generated by a NATO element or national information generated by a NATO member nation. If it has been marked "NATO" by the originating nation, it must be assumed to contain information released to NATO, and it is controlled under the NATO Security Program. B. If the material has a national classification marking and is not marked "NATO" by the originator, DO NOT apply a NATO marking unless you are informed in writing by the originator that the material is intended for NATO and is to be protected under the NATO Security Program. Moreover, the material or the information therein shall not be released into the NATO system without the prior written consent of the originator.
17.b. WHAT ARE THE FOUR LEVELS OF NATO CLASSIFIED INFORMATION?	A. NATO has four levels of classified information: • COSMIC TOP SECRET

TOPIC	PERSONALIZATION
	• NATO SECRET • NATO CONFIDENTIAL • NATO RESTRICTED. B. Certain NATO information is further categorized as ATOMAL information. NATO also distinguishes official, unclassified information.
17.c. WHAT IS NATO UNCLASSIFIED?	A. NATO UNCLASSIFIED (NU) - This marking is applied to official information that is the property of NATO, but does not meet the criteria for classification. B. Access to the information by non-NATO entities is permitted when such access would not be detrimental to NATO. In this regard, it is similar to U.S. Government official information that must be reviewed prior to public release.
17.d. HANDLING U.S. CLASSIFIED DOCUMENTS THAT CONTAIN NATO CLASSIFIED INFORMATION.	A. A newly generated U.S. classified document that contains NATO classified information shall bear a U.S. classification marking that reflects the highest level of NATO or U.S. classified information it contains. B. Declassification and downgrading instructions shall indicate that the NATO information is exempt from downgrading or declassification without the prior consent of NATO; the reason to be cited is ”foreign government information.” The statement “THIS DOCUMENT CONTAINS NATO CLASSIFIED INFORMATION” will be affixed to the front cover or first page, if there is no cover. C. Portions that contain NATO classified information shall be marked to identify the information (e.g., NS). D. The document shall be accounted for, safeguarded and controlled as specified for NATO documents of the same classification.

TOPIC	PERSONALIZATION
	The physical security requirements for material marked NATO CONFIDENTIAL and above are the same as for U.S. material of the same level of classification. E. NATO RESTRICTED material may be stored in a locked filing cabinet, book case, desk or other such container, or in a room or building that is locked during non-duty hours, provided access to the room or building is controlled so that only authorized personnel can gain access to the information.
17.e. STORING NATO INFORMATION.	A. All personnel with access to a security container that is used to store NATO information must be briefed and authorized access to the level and type of NATO information that is stored in that container. B. NATO guidelines are very similar to those used for U.S. material. C. NATO material can be stored in the same security container as non-NATO information provided the NATO material is physically separated from non-NATO material by at least a file divider. *[Reference AFI 31-401, para 5.1.]*
17.f. WHAT TO DO WHEN YOU FIND NATO INFORMATION IS NOT PROPERLY PROTECTED.	A. If you find NATO material unsecured and unattended, immediately contact your supervisor, security manager, commander or registry system official. Stay with the material and wait for the security manager or registry official to arrive. B. Do not disturb the area or material. Do not allow anyone else to disturb the area or allow unauthorized personnel to have access to the material. C. If it is necessary that you leave the area before your security manager or registry system official can assume custody, place the material in a security container and lock

TOPIC	PERSONALIZATION
	the container. If the container is already locked, and you are not authorized access, or there is no container, take the material directly to an appropriately cleared security or registry system official, explain the circumstances and obtain a receipt for the material. D. The servicing subregistry or control point must be informed of the incident, in addition to the responsible security or counterintelligence officials

APPLICATION: N/A

EVALUATION: N/A

CONCLUSION

Using the elements of attention, motivation and review; conclude the subject of cleared personnel initial training.